[illegible]

www.huawei.com

[illegible] © 2018 [illegible]

[illegible]

- [illegible]“[illegible]”[illegible]
- [illegible] USG [illegible]

[illegible]

- [illegible]
  - [illegible]
  - [illegible]

[illegible] © 2018 [illegible]

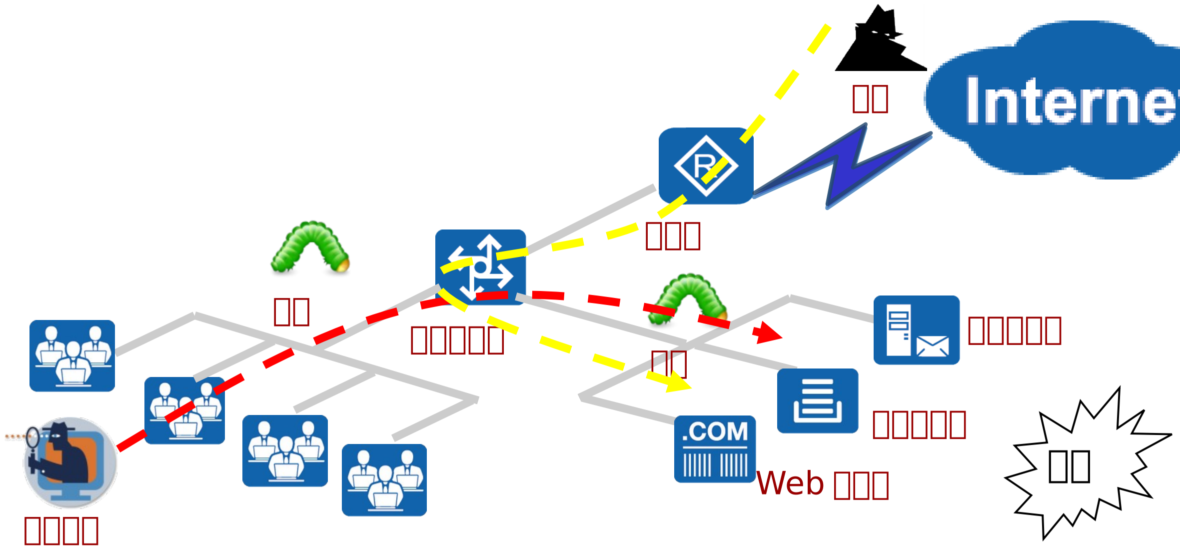
[illegible]

1. [illegible]
2. [illegible]
3. [illegible]

[illegible] © 2018 [illegible]

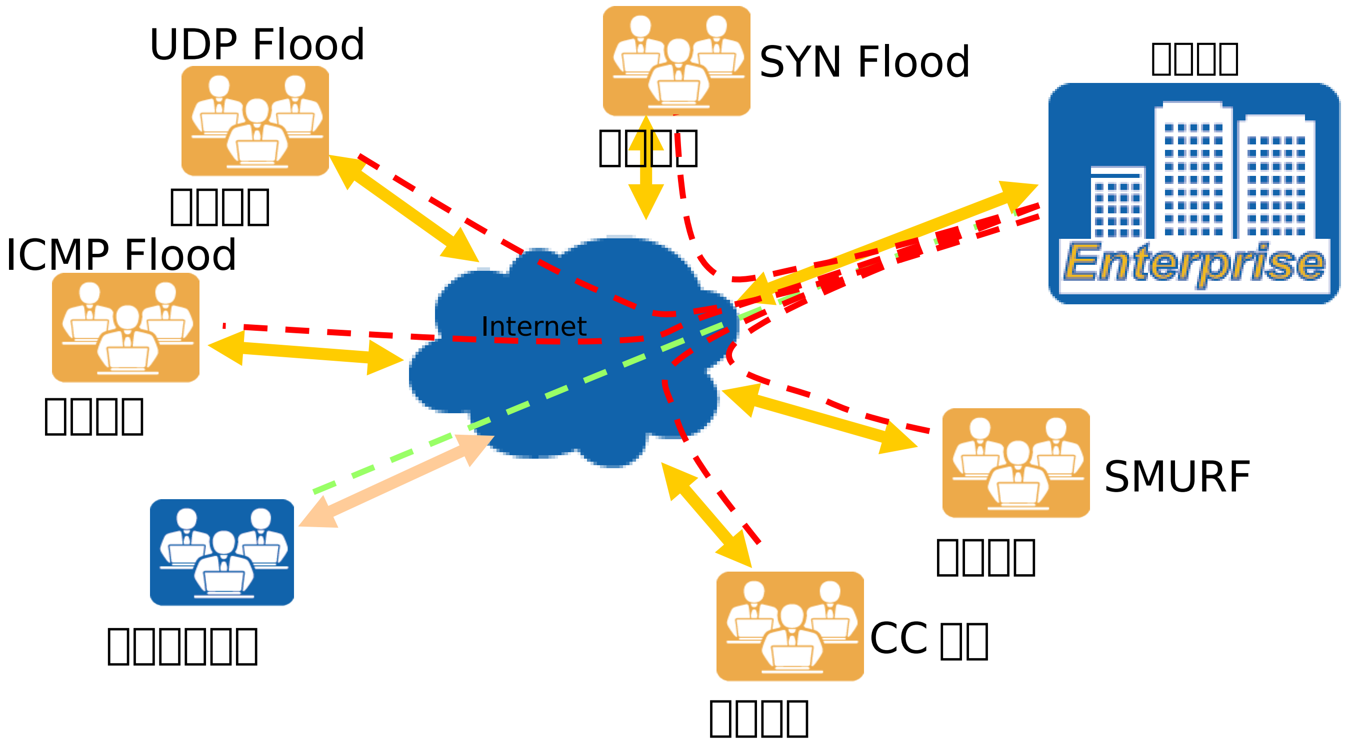
[illegible]

- [illegible]


Internet
.COM
Web [illegible]

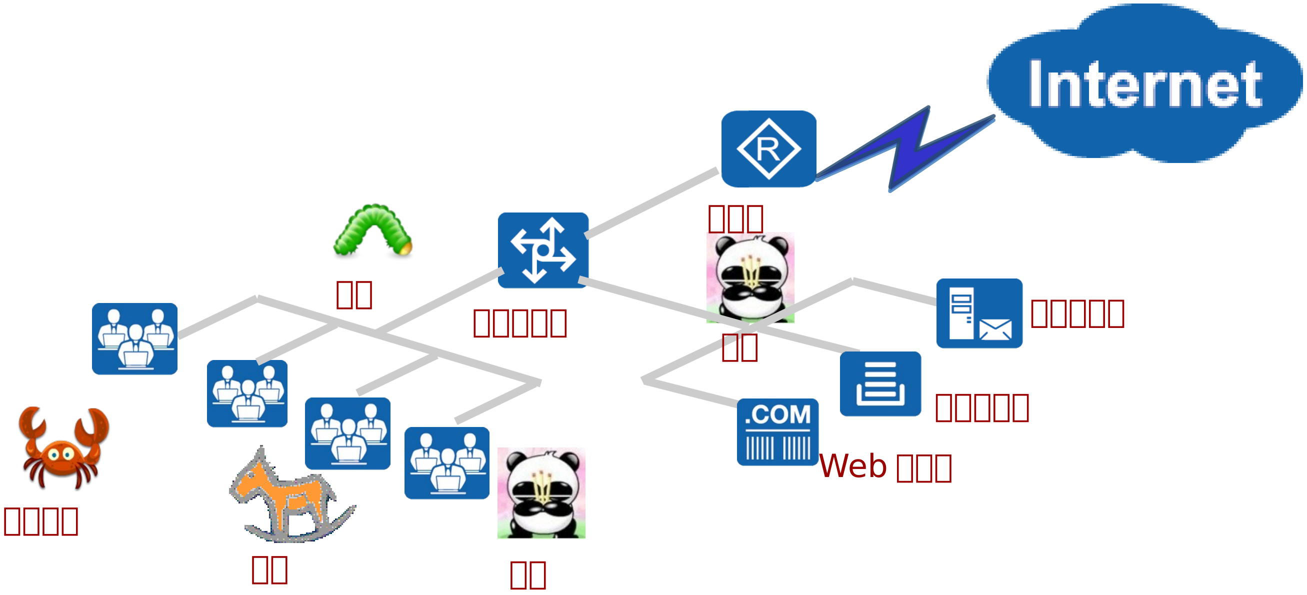
[illegible]

- [illegible] DDOS [illegible]


UDP Flood
SYN Flood
ICMP Flood
Internet
Enterprise
SMURF
CC

□□□□□□□□□□□

- □□□□□□□□□□□□□□□□□□ IT □□□□□□□□□□□□□□□□□□□□□□□□
  □□□□□□□□□□□□□□□



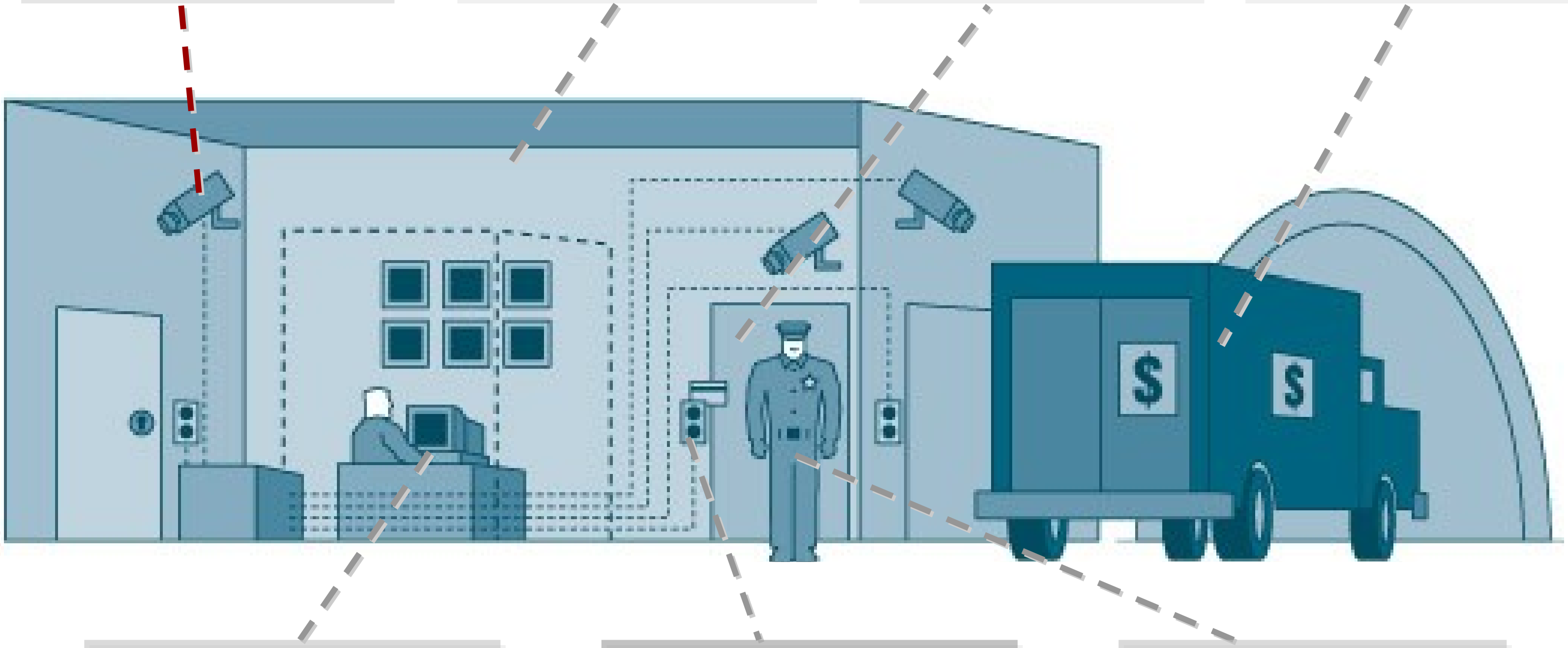
	√	√	√
	√		√
	√	√	√

[illegible]

1. [illegible]

2. [illegible]

3. [illegible]

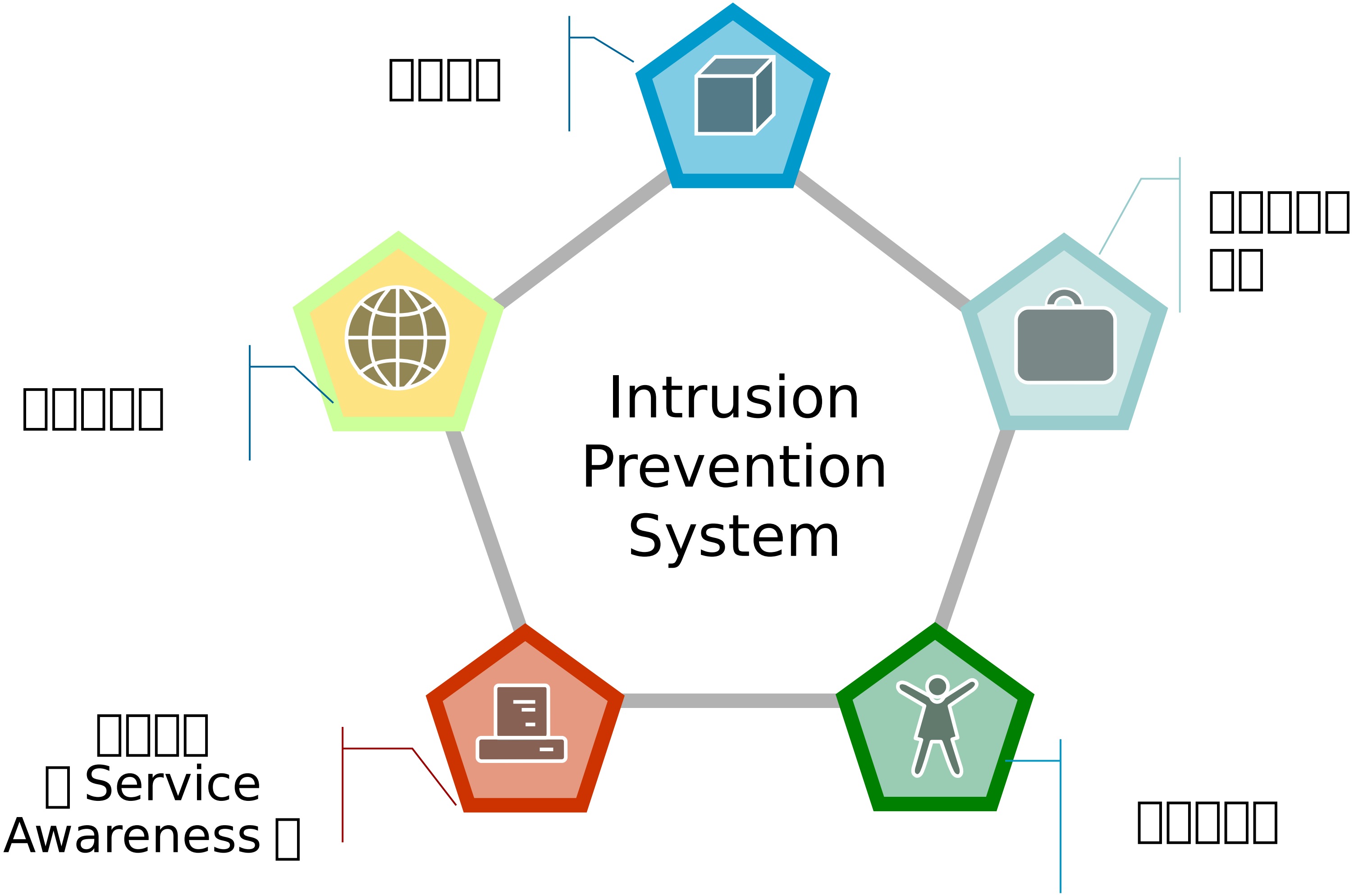

VPN

[illegible]

- [illegible] IPS [illegible] Intrusion Prevention System [illegible]
- IPS [illegible]

[illegible]	[illegible]
[illegible]	[illegible]

[illegible]



[illegible]
[illegible]
[illegible]
Intrusion Prevention System
[illegible]
[illegible]（Service Awareness）
[illegible]

[illegible]

日志
流量日志
威胁日志
URL日志
操作日志
系统日志
威胁日志列表
导出
列定制
查看
时间
威胁类型
风险等级
威胁ID
威胁名称
2018/07/05 10:41:45
入侵
低
1540
Cisco公共服务框架Help Servlet..
查看威胁日志详情（入侵）
日志公共字段
时间: 2018/07/05 10:41:45
协议: TCP
安全策略: untrust_trust
应用类别: 网络架构
应用子类别: 网络基础协议
应用: HTTP
威胁
威胁类型: 入侵
入侵子类型: 攻击入侵
威胁名称: 跨站脚本攻击尝试 - 存在于HTTP
威胁ID: 2000120
威胁计数: 1
配置文件: strict
动作: 告警
严重性: 中
风险等级: 低
目标类型: 服务端
操作系统: all
攻击分类: XSS
访问内容: /cwhp/device.center.do?device=
源
源安全区域: untrust
源地区: 未知区域
源地址: 172.16.8.47
源端口: 2882
目的
目的安全区域: trust
目的地区: 未知区域
目的地址: 172.16.8.102
目的端口: 1741

[illegible] © 2018 [illegible]

[illegible]

1. [illegible]
2. [illegible]
3. **[illegible]**

[illegible] © 2018 [illegible]

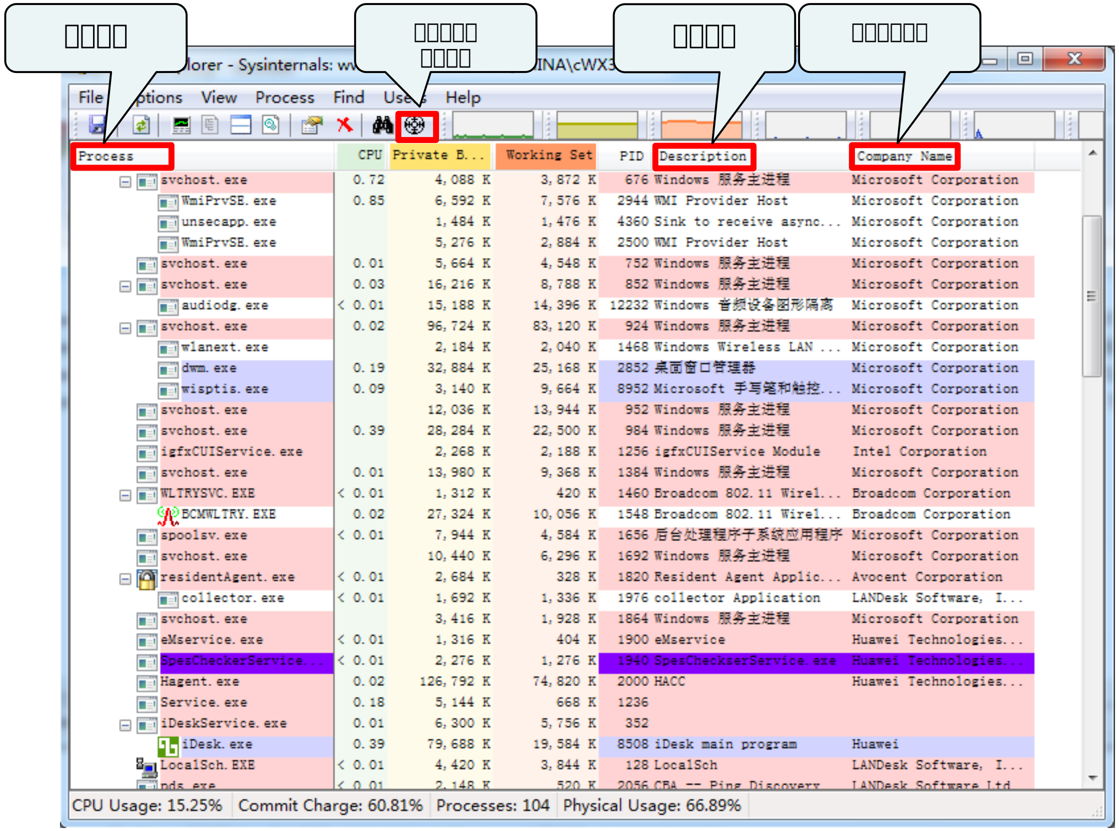
[illegible]

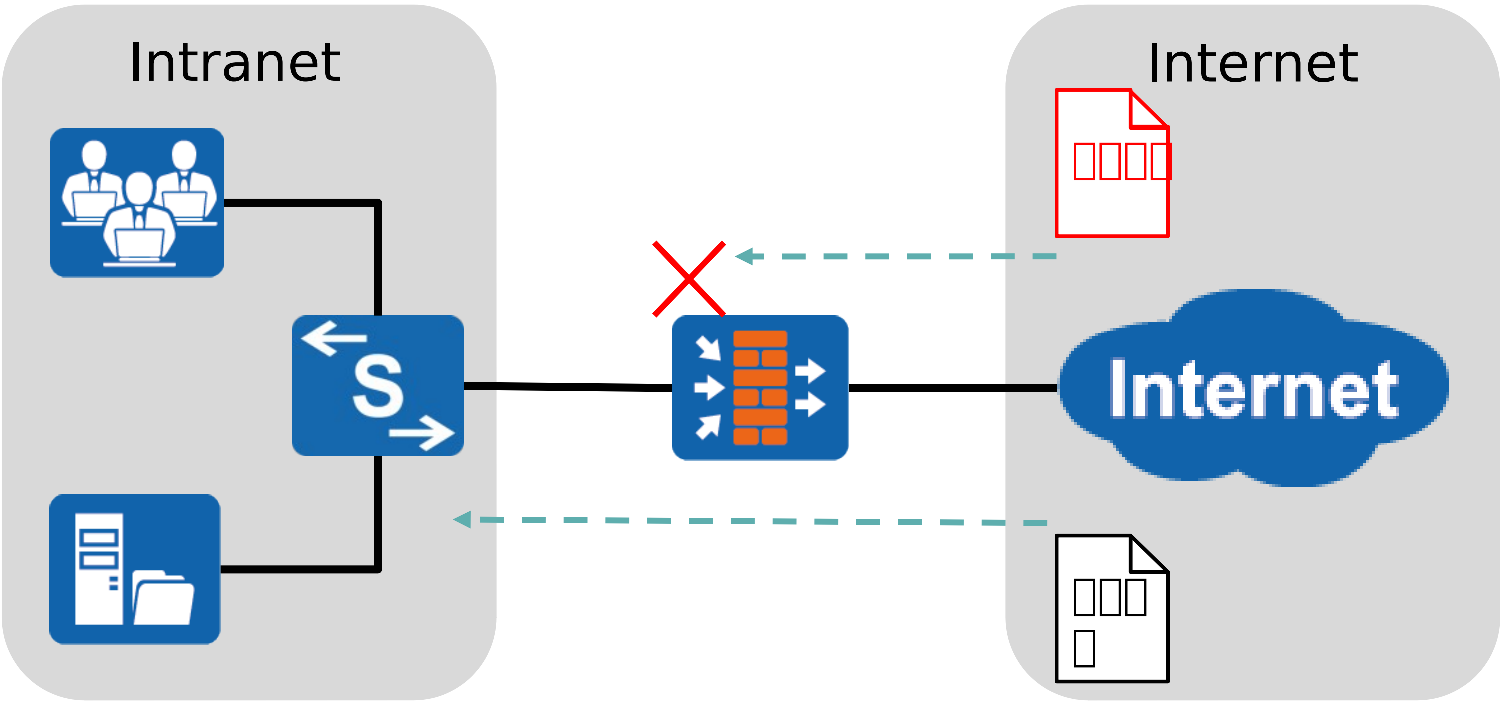
- [illegible]
  - [illegible] Computer Virus [illegible]
- [illegible]
  - [illegible]

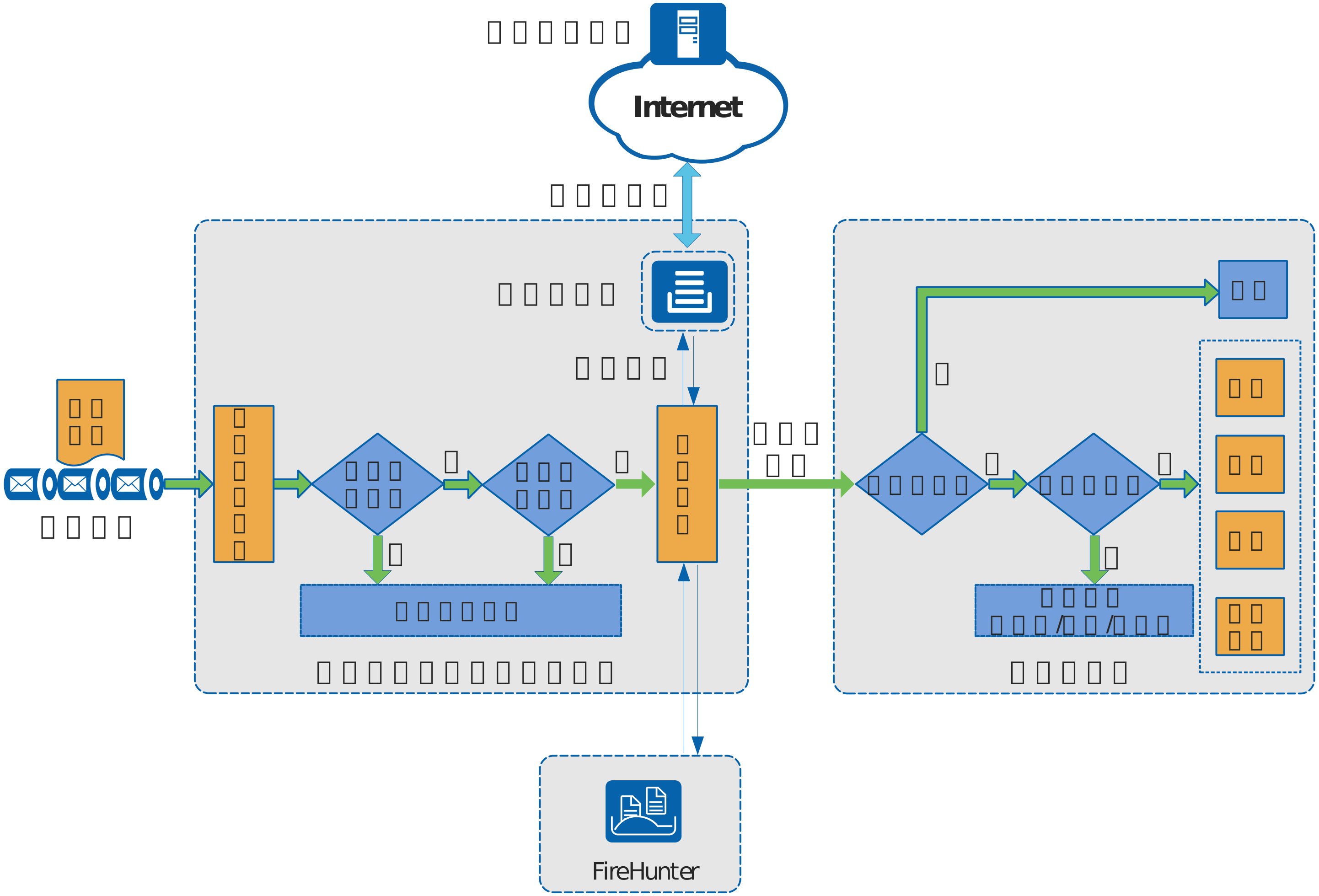
[illegible]

[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible] (Patch)	[illegible]

[illegible] © 2018 [illegible]


File Options View Process Find Users Help
Process
CPU
Private B...
Working Set
PID
Description
Company Name
CPU Usage: 15.25%
Commit Charge: 60.81%
Processes: 104
Physical Usage: 66.89%


Intranet
Internet
Internet



© 2018

[illegible]

日志
流量日志
威胁日志
URL日志
操作日志
系统日志
查看威胁日志详情（病毒）
日志公共字段
时间: 2018/07/23 15:10:48
协议: TCP
安全策略: IDS_test
应用类别: 网络架构
应用子类别: 网络基础协议
应用: HTTP
威胁
威胁类型: 病毒
威胁名称: EICAR.Test.FILE.1
威胁ID: 16424404
威胁计数: 1
配置文件: av
动作: 告警
文件名称: eicar_com.zip>eicar.com
文件类型: com
访问内容:
Hash值: 267D772D8ED87333
源
源安全区域: untrust
源地区 未知区域
源地址: 10.1.2.100
源端口: 80
目的
目的安全区域: trust
目的地区 未知区域
目的地址: 10.1.1.100
目的端口: 49396
libai@security.com
发给 dufu
2017-07-13 10:03 ????
eicar_com.zip (0 B)
Warning:
eicar_com.zip is deleted from the mail because it contains virus.

[illegible]

1. [illegible]SMTP[illegible]
   - A. [illegible]
   - B. [illegible]
   - C. [illegible]
   - D. [illegible]
2. [illegible]
   - A. IPS[illegible]
   - B. IPS[illegible]
   - C. [illegible]
   - D. IPS[illegible]

[illegible]© 2018 [illegible]

[illegible]

- [illegible]
- [illegible]
- [illegible]IDS[illegible]IPS
- [illegible]

[illegible]

www.huawei.com